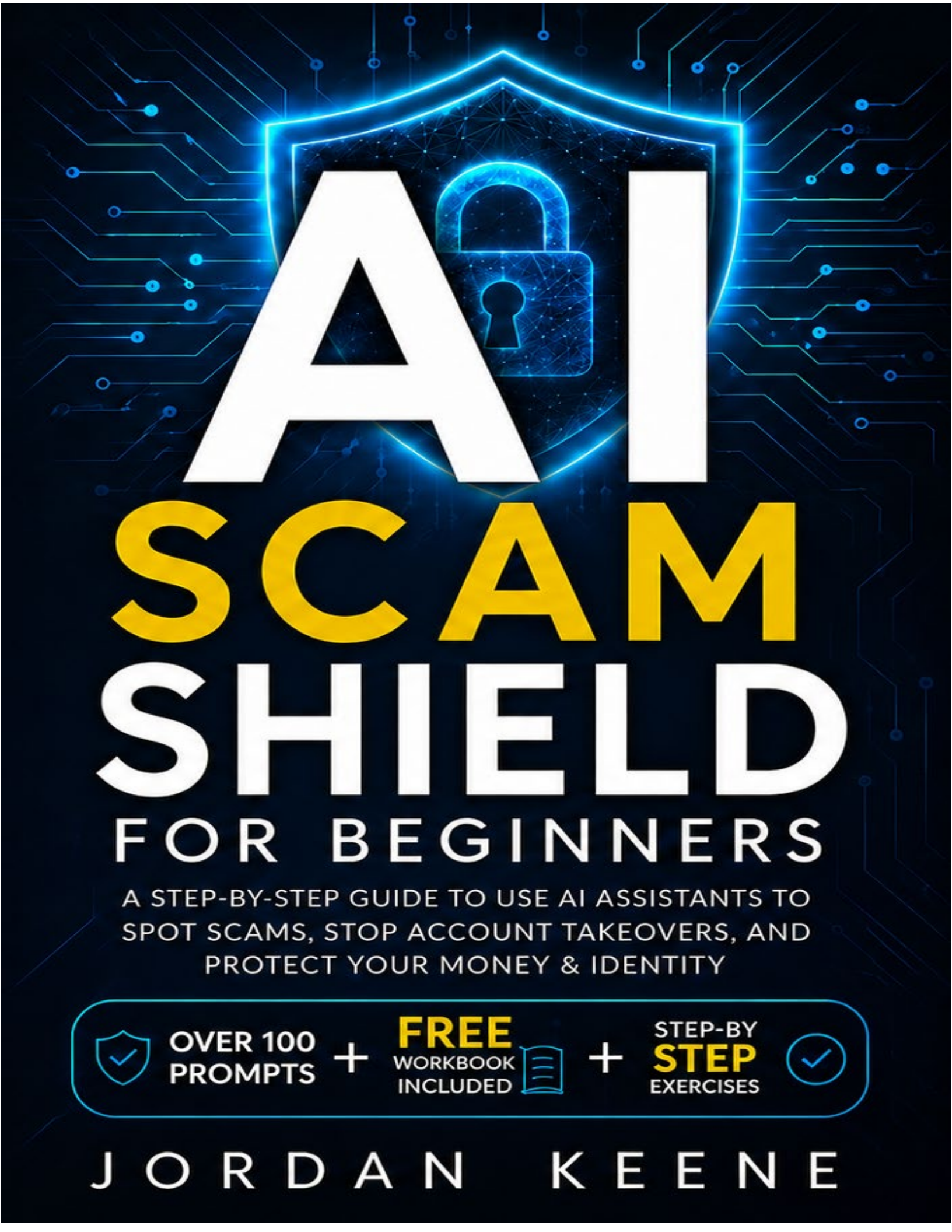
AI
SCAM
SHIELD
FOR BEGINNERS
A STEP-BY-STEP GUIDE TO USE AI ASSISTANTS TO SPOT SCAMS, STOP ACCOUNT TAKEOVERS, AND PROTECT YOUR MONEY & IDENTITY
OVER 100 PROMPTS
+
FREE WORKBOOK INCLUDED
+
STEP-BY STEP EXERCISES
JORDAN KEENE

Workbook for the AI Scam Shield for Beginners

Disclaimer

This workbook is intended for educational and informational purposes only. It is designed to help readers reflect, organize ideas, practice new skills, and apply the concepts presented in the accompanying book or program.

The information, exercises, prompts, checklists, and activities included in this workbook are not a substitute for professional advice, diagnosis, treatment, or services. Readers should consult a qualified professional when making decisions related to health, mental health, legal matters, finances, business, safety, caregiving, or other specialized concerns.

Individual results may vary. The author and publisher make no guarantees regarding specific outcomes and are not responsible for any loss, injury, damage, or consequences resulting from the use or misuse of this workbook.

Some activities may require personal judgment, additional research, or professional guidance. Always verify important information, protect your privacy, and use tools, technology, and recommendations responsibly.

By using this workbook, you acknowledge that you are responsible for your own decisions, actions, and results.

Table of Content

Introduction to the Case Study Workbook... 1

Case Study (Chapter 1): “The Bank Fraud Text That Tries to Rush You” 3

Case Study (Chapter 2): “The Scary Bank Email—How to Use AI *Safely* Without Oversharing” 11

Case Study (Chapter 3): “The Unexpected MFA Prompt—How Your 80/20 Baseline Stops a Takeover” 19

Case Study (Chapter 4): “The Toll Text Scam—Running the 5-Step AI Scam Check Workflow” 27

Case Study (Chapter 5): “The ‘Bank Fraud Department’ Call—How to Beat Spoofing and Deepfakes” 35

Case Study (Chapter 6): “The ‘Friend’ DM + Marketplace Payment Screenshot Scam”.. 43

Case Study (Chapter 7): “Email Takeover Attempt—Lock Down the Master Key Before It Spreads” 53

Case Study (Chapter 8): “My Phone Lost Service—Is This a SIM Swap?” 61

Case Study (Chapter 9): “The Subscription Renewal Email—How to Protect Money, Set Alerts, and Dispute Fast” 70

Case Study (Chapter 10): “A New Credit Inquiry You Don’t Recognize—Monitoring vs. Freeze + Identity Defense Folder” 80

Case Study (Chapter 11): “A Transfer You Don’t Recognize—First 15 Minutes / First 24 Hours” 88

FIRST 15 MINUTES (Stop More Harm) 88

EVIDENCE CAPTURE (Do this while fixing, not after) 91

AVOID THE “SECOND SCAM” (Most people get hit here) 91

FIRST 24 HOURS (Stabilize So It Doesn’t Echo) 92

FIRST 15 MINUTES (Stop the Bleeding) 94

EVIDENCE CAPTURE (Quick and Practical) 96

AVOID THE “SECOND SCAM” 97

FIRST 24 HOURS (Stabilize) 97

Case Study (Chapter 12): “From Overwhelmed to Protected—Running the 30-Day AI Scam Shield Plan” 99
Week 1 (Days 1–7): Email + Password Manager + MFA 99
Week 2 (Days 8–14): Phone + Carrier + Cleanup 100
Week 3 (Days 15–21): Money Rules + Alerts + Habits 101
Week 4 (Days 22–30): Credit/Identity + Family Plan + Drill..... 102
Week 1: Email + Password Manager + MFA 105
Week 2: Phone + Carrier Protections + Cleanup 106
Week 3: Money Rules + Alerts + Routine . 107
Week 4: Credit/Identity + Family Pact + Drill 108
Conclusion..... 110

Introduction to the Case Study Workbook

Welcome to the **AI Scam Shield for Beginners Case Study Workbook**—your hands-on companion to the main book.

Reading about scams is helpful, but **practicing what to do** is what builds real confidence. This workbook gives you realistic, easy-to-follow case studies that walk you through the exact systems taught in each chapter—so when a suspicious text, email, or phone call shows up in real life, you won't freeze or guess. You'll know the next step.

Each case study is designed to feel like a "real moment" you could experience: a bank alert text, a fake invoice email, a spoofed phone call, a marketplace scam, or an identity theft warning. You'll work through the situation using the same method the book teaches—like identifying what the scammer wants (money, accounts, identity, or access), spotting the "emotion hack," using **Pause–Verify–Decide**, and verifying through official channels you choose.

You'll also see how to use **AI assistants safely** as a calm helper—not a truth machine—without pasting private or sensitive information. The goal is not to become paranoid or technical. The goal is to build a repeatable habit: **slow down, verify, and act with confidence.**

How to Use This Workbook

- **Option 1: Follow along chapter-by-chapter.** Read a chapter in the book, then complete the matching case study here.
- **Option 2: Jump to the scenario you're facing.** If you're dealing with a phone scam, start with Chapter 5's case study. If you're worried about identity theft, go to Chapter 10.
- **Option 3: Practice as a family.** These are excellent for parents, teens, and older relatives—especially the code word plan and call-back rules.

What You'll Gain

By the end of this workbook, you'll be able to:

- Recognize scam patterns quickly (even when they look convincing)
- Use a simple system to verify messages without panic
- Protect your accounts and money with practical "80/20" steps
- Respond calmly if something goes wrong using a clear action order

You don't need to be perfect to be safe. You just need a plan you can run—even on a stressful day. Let's build that plan together.

Case Study (Chapter 1): “The Bank Fraud Text That Tries to Rush You”

The Situation

It’s 7:42 p.m. You’re cleaning up after dinner when your phone buzzes.

Text message (example):
“[Bank]: URGENT—Unusual login detected. Your account will be locked tonight. Verify now: [LINK]”

Your stomach drops. The message feels believable because you bank online and it sounds serious. This is exactly the kind of “modern scam environment” that hits people through everyday channels like texts and urgent alerts.

Step 1: Name What the Scammer Wants (The “4 Goals” Check)

Before you do anything, ask: **What are they after?** Chapter 1 teaches that scams usually aim for **money, accounts, identity, or access**.

In this message, the likely target is:

- **Accounts** (getting your login) and/or
- **Money** (getting you to “confirm” something that leads to theft)

Just naming the target helps you shift from *reacting* to *thinking*.

Step 2: Spot the Emotion Hack

This message pushes emotional buttons on purpose. Chapter 1 explains scammers “hijack” emotions—especially urgency and fear—so you act fast without verifying.

Emotion hack signals in the message:

- **Urgency:** “URGENT… tonight”
- **Fear:** “account will be locked”
- **Pressure:** “verify now”

This is your cue that the message is trying to move you into “fast mode,” not “safe mode.”

Step 3: Use the Chapter 1 Habit — No Action While Emotional

Chapter 1’s core protective habit is simple: **no action while emotional**, using a mini routine: **Pause** → **Breathe** → **Verify**.

A) PAUSE (10 seconds)

- Put the phone down.
- Do **not** click the link.
- Do **not** reply.

B) BREATHE (10–20 seconds)

Take 2–3 slow breaths. The goal is to step out of fight-or-flight so you can choose a smart next step.

C) VERIFY (change the channel)

Chapter 1 is clear: verify through **official channels you choose**, not the channel the message gives you.

Step 4: Use AI the Right Way (Calm Helper, Not a Truth Machine)

Chapter 1 explains AI can be a **second set of eyes** that helps you slow down and notice red flags—but it **can’t guarantee** a message is real, and you should verify with official sources.

What you do:

1. **Sanitize** the message (remove the link and personal details).
2. Ask your AI assistant:
    - "List red flags in this message."
    - "What are the safest verification steps that don't use the link?"

This uses AI as a calm coach—exactly as intended in Chapter 1.

Step 5: Verify Through Official Channels (Not the Text)

Now you verify safely:

Safe verification options (choose one):

- Open your **bank's official app** (the one you already use) and check alerts.
- Call the **number on the back of your card** (not any number in the text).
- Type your bank's website yourself (or use a bookmark), then check messages/alerts.

What happens in this case study

You open the bank app—**no alerts**.
You call the number on your card—your bank confirms: **no lock, no urgent login event**.

That's the moment you know: the text was designed to rush you into a fake login page.

Step 6: Decide (Clean Exit)

Based on Chapter 1's guidance (verify first, then decide), your best move is:

- Delete the message

- Mark as junk/report if your phone allows
- Continue your day—without panic

You didn't "outsmart" the scam. You followed the system: identify the goal, recognize the emotion hack, pause, and verify.

Quick "Follow This Next Time" Summary (1 Minute)

1. **What do they want?** money / accounts / identity / access
2. **What emotion are they pushing?** urgency/fear/authority/shame
3. **No action while emotional:** Pause → Breathe → Verify
4. **AI helps you slow down** (but doesn't verify for you)
5. **Verify through official channels you choose**

Case Study (Chapter 1) — Meet Tanya Rivera: The “Package Delay” Text

Who Tanya Is

Tanya Rivera is a 38-year-old working parent who manages most of her life on her phone—school emails, online shopping, banking, and appointments. She’s smart and careful, but she’s busy, and she’s exactly the kind of person scammers target when she’s tired and distracted.

The Moment

At 6:14 p.m., Tanya gets a text from an unknown number:

“USPS: Your package has been delayed due to an address issue. Click here to update delivery details: [LINK]”

Tanya’s first thought is, *“Oh no… I did order something.”* Her second thought is, *“I should fix this before it gets returned.”* That feeling—rushed, slightly anxious—is the doorway scammers want.

Step 1: Tanya Identifies What the Scammer Wants

Chapter 1 says nearly every scam is trying to get **money, accounts, identity, or access**. Tanya asks herself:

- **Money?** Maybe a “small redelivery fee”
- **Identity?** Address, name, possibly DOB
- **Account access?** A login or payment page
- **Device access?** Less likely from a delivery text

She realizes: *This could be money + identity.* That clarity alone slows her down.

Step 2: Tanya Spots the “Emotion Hack”

Chapter 1 explains scammers “hack” emotions like **urgency, fear, authority, confusion, and shame** to shut down thinking. Tanya notices:

- **Urgency:** “delayed” + “update now”
- **Authority:** “USPS” branding
- **Fear:** losing a package

Her heart rate goes up. That’s her signal: *emotion means pause.*

Step 3: Tanya Uses the New Habit — “No Action While Emotional”

Chapter 1 teaches a mini routine: **Pause** → **Breathe** → **Verify**. Tanya does it exactly:

A) Pause (10 seconds)

She puts her phone down and does not tap the link.

B) Breathe (10–20 seconds)

Two slow breaths. Enough to get out of “react mode.”

C) Verify (change the channel)

Tanya reminds herself: *If it’s real, it will still be real in 10 minutes.*

Step 4: Tanya Uses AI the Right Way (Second Set of Eyes)

Chapter 1 says AI can help as a calm assistant—but it can’t guarantee truth. Tanya uses AI to slow down and spot patterns, without sharing private info.

She pastes a **sanitized** version (no link, no personal info) and asks:

“Analyze this message for scam red flags and tell me what to verify safely without clicking links.”

The AI points out common red flags: urgency + unknown number + link-based “address update” request.

Step 5: Tanya Verifies Through Official Channels

Chapter 1’s verification principle: **don’t trust links or numbers in the message; verify using official channels you find yourself.**

Tanya does this:

- She opens her shopping app and checks **order tracking** (no mention of USPS address issue).
- She goes to the official USPS site by typing it herself (or uses a trusted app), and enters tracking numbers she already has.

Result: **No package problem exists.**

Step 6: Tanya Decides (Calm Exit)

Now she can decide without fear:

- Deletes the text
- Marks it as spam/junk
- Moves on with her night

She didn’t need to be a cybersecurity expert. She just followed the Chapter 1 system: identify the goal, spot the emotion hack, and verify in a channel she controls.

What Tanya Learned (Chapter 1 in One Line)

Scams don’t beat intelligence—they beat urgency. Your job is to slow the moment down.

Case Study (Chapter 2): “The Scary Bank Email—How to Use AI *Safely* Without Oversharing”

This case study is built to help the reader practice Chapter 2’s core system: **AI is powerful, but not a vault**, **never paste secrets**, **redact with placeholders**, use the **Safe Prompt Formula**, and follow the **Verification Rule (AI suggests; you verify)**.

The Situation

You open your email and see a subject line like:

“URGENT: Account Locked — Verify Identity Now”

The email includes details like your name, the last 4 digits of an account, and a link. It asks you to “confirm” your information immediately.

Your instinct is to forward the whole email to an AI assistant and ask, “Is this real?” Chapter 2 says that’s where people accidentally create risk—by oversharing sensitive data into a chatbot.

Step 1: Apply the #1 Rule — Never Paste Secrets

Before you paste anything into an AI tool, you stop and check for “secret” data: passwords, codes, account numbers, full SSN, full card numbers, and anything that could unlock money or identity.

What you do right now:

- You **do not** paste the email as-is.
- You **do not** paste links.
- You **do not** paste any account identifiers beyond general info.

This matches Chapter 2's blunt rule: **never paste secrets into a chatbot.**

Step 2: Use the Simple Redaction Method (Placeholders)

Chapter 2 teaches a simple redaction workflow: **scan → replace sensitive info with placeholders → tell the AI you did it**.

Redaction (example)

You rewrite the email like this:

Sanitized version (safe to share):
"Email claims my account at [BANK_NAME] is locked due to 'suspicious activity' and wants me to verify identity using a link: [SUSPICIOUS_LINK]. It references an account ending in [LAST_4_DIGITS]. Sender: [EMAIL_ADDRESS]."

This preserves meaning while removing identifying details, exactly like the Chapter 2 examples.

Step 3: Use the Safe Prompt Formula (Role–Task–Context–Constraints–Output)

Now you ask your AI assistant for help using the five-line framework in Chapter 2.

Copy/paste prompt (tool-agnostic):

Role: Act as a cautious cybersecurity assistant for everyday consumers.
Task: Help me understand whether this redacted email shows warning signs of a scam.
Context: Here is the redacted message: [PASTE REDACTED TEXT].
Constraints: Do not ask for passwords, codes, or full account numbers. Do not tell me to click links.

Output: Give me red flags in plain language + 3 safe next steps + a short script I can use.

Step 4: Ask AI for the "Right Kind" of Help (Clarity, Not Panic)

Chapter 2 recommends using AI for **red flags, next steps, and scripts**—not certainty.

A solid AI response would likely include:

- Red flags (urgency language, link-based "verification," sender mismatch possibilities)
- Next steps (log in through official app, contact bank using trusted number)
- Script (what to say to the bank)

And it should warn you away from prompts like "Is this 100% real?" because AI can't guarantee that.

Step 5: Follow the Verification Rule (Non-Negotiable)

Even with a great AI analysis, Chapter 2 draws a hard line: **AI can suggest; you must verify.**

So you verify like this (not using anything in the email):

- Open your **bank's official app** (the one you already use) and check alerts.
- Or type the bank's official URL yourself / use a bookmark you trust.
- Or call the **customer service number on the back of your card** or statement.

Chapter 2 also drills the key phrase: **never trust contact info in the message** (numbers, links, QR codes, look-alike emails).

The Outcome (What Happens in This Case)

You open your bank's official app. There is **no account lock** and **no security alert**.
You call the number on your card. The representative confirms: **the email is not from the bank**.

You delete the message (and optionally report it), and you did it without ever handing your personal data to a chatbot or clicking a risky link.

Quick "Do This Next Time" Summary

1. **Never paste secrets** into AI.
2. **Redact with placeholders** before sharing text.
3. Use the **Safe Prompt Formula** to get red flags + safe steps.
4. Follow the **Verification Rule:** verify through official channels you initiate.

Case Study (Chapter 2) — Meet Marcus Lee: Using AI Safely Without Oversharing

Who Marcus Is

Marcus Lee is a 44-year-old project manager who's new to AI but loves the idea of using it for quick clarity. He's careful with money, but he's also the kind of person who will copy/paste an entire email to "just get an answer" when he's stressed—exactly what Chapter 2 teaches you *not* to do.

The Moment

At 9:07 a.m., Marcus opens his inbox and sees a scary email:

Subject: "Security Alert: Account Locked — Action Required"
The email says his bank account has been locked and includes a button: **"Verify Now"** and asks him to confirm details immediately.

Marcus's first instinct: paste the whole email into an AI assistant and ask, "Is this real?"

Chapter 2 stops him right there with one key idea: **AI is powerful, but it is not a vault.**

Step 1: Marcus Uses the #1 Rule — Never Paste Secrets

Before he pastes anything, Marcus scans the email for "secrets" Chapter 2 warns about:

- passwords, one-time codes, account numbers, full SSN, full card numbers, address + DOB combos, and private links.

He notices the email contains:

- a link/button,
- partial account details,
- and language pressuring him to act now.

So he does NOT paste it as-is.
That single decision prevents a bad habit: turning AI into a place where sensitive information could live long-term.

Step 2: Marcus Uses the Simple Redaction Method (Placeholders)

Chapter 2 teaches a simple method: replace sensitive info with placeholders so AI can help without exposing you.

Marcus creates a sanitized version like this:

“Email claims my account at [BANK] is locked due to suspicious activity and asks me to verify identity using [LINK_REMOVED]. It references account ending in [LAST4]. Sender is [EMAIL_ADDRESS].”

He keeps the meaning, removes the risk.

Step 3: Marcus Uses the Safe Prompt Formula

Chapter 2 gives Marcus a reliable format: **Role** → **Task** → **Context** → **Constraints** → **Output**.

He pastes this:

Role: Act as a cautious cybersecurity assistant for everyday consumers.
Task: Identify scam red flags in this redacted email and help me respond safely.
Context: Redacted message: [PASTE SANITIZED TEXT].
Constraints: Do not ask for passwords, codes, or account numbers. Do not tell me to click any links.

Output: Give me a risk rating, the top red flags, and 3 safe verification steps.

This is exactly how Chapter 2 wants readers to use AI: structured, calm, and privacy-first.

Step 4: Marcus Asks AI for the Right Kind of Help (Clarity, Not Certainty)

Chapter 2 warns against chasing “100% real or fake” certainty. Instead, Marcus asks for:

- **red flags**
- **safe next steps**
- **scripts** (what to say to support)

The AI points out likely issues:

- urgency language,
- link-based verification,
- and the risk of a look-alike sender domain.

But it also reminds him: **AI can’t verify it for sure.**

Step 5: Marcus Follows the Verification Rule (Non-Negotiable)

Chapter 2 makes this rule crystal clear: **AI suggests; you verify through official channels you find yourself.**

Marcus verifies safely by:

1. Opening his bank’s **official app** (not the email link)
2. Checking for alerts inside his account
3. If needed, calling the number on the **back of his card** (not any number in the email)

Outcome: There is no lock, no fraud alert, and no message inside the bank app.
The email was a trap designed to get him to click.

Step 6: Marcus Takes the "Smart Exit"

Marcus:

- Deletes the email,
- Marks it as spam/phishing,
- And spends 2 minutes turning on (or checking) MFA for his email and bank later—because now he's thinking proactively.

He used AI exactly the way Chapter 2 teaches: **as a clarity tool, not a vault, and not a judge.**

What Marcus Learned (Chapter 2 in One Line)

You can use AI for help without feeding it your private life—redact first, ask for safe steps, and verify through official channels.

Case Study (Chapter 3): “The Unexpected MFA Prompt—How Your 80/20 Baseline Stops a Takeover”

This case study helps the reader practice Chapter 3’s system: focus on the **Top 5 accounts**, use **unique passwords + a password manager**, turn on **MFA with the simple ranking**, tighten **recovery options**, and keep everything stable with the **Weekly 10-Minute Habit**.

The Situation

It’s a normal weeknight. You’re making dinner when your phone buzzes:

“Your email account sign-in code is: 482193”
(or a push prompt like: **“Are you trying to sign in?”**)

You weren’t logging in. This is exactly the kind of moment Chapter 3 prepares you for: **unexpected MFA prompts are an alarm bell**, not an annoyance.

Step 1: Identify Which “Front Door” Is Under Attack

Chapter 3 explains the 80/20 baseline: lock down the small set of accounts that matter most—especially **email**, because it can lead to resets for everything else.

Top 5 quick check (from the book’s baseline):

1. Email
2. Banking / credit cards
3. Phone carrier

4. Password manager
5. Primary social

The MFA prompt suggests someone may have your **email password**, and is trying to get past your second lock.

Step 2: Follow the "Approve Only When You Initiated It" Rule

Chapter 3 gives a simple habit: **only approve MFA prompts when you initiated them.** If you didn't, you treat it as a likely attack and move into "containment mode."

What you do:

- You do **not** approve.
- You do **not** reply with any code (ever).

Step 3: Use Your Password Manager to Reset the Email Password (Fast + Clean)

Chapter 3 recommends using a password manager and focusing on your **first 10 logins** (including your main email and bank), changing them to strong unique passwords and saving them in the vault.

What you do (5 minutes):

1. Open your password manager.
2. Generate a new strong password for your email.
3. Change your email password immediately.
4. Save it to the vault.

This instantly breaks the attacker's "stolen password" attempt.

Step 4: Check Recovery Options (Because Recovery Is a Hidden Back Door)

Chapter 3 warns that recovery settings can become a back door if they're outdated—old numbers, old emails, or old devices can let attackers regain access later.

What you do next (5 minutes):

- Review recovery email + phone: remove anything old.
- Confirm backup codes exist and are stored safely.
- Check your "trusted devices/sessions" list and remove unknown devices.

Step 5: Upgrade MFA (Use the Simple Ranking)

Chapter 3 gives a beginner-friendly MFA ranking: **passkeys/security keys (best) → authenticator app/prompt (good) → SMS (last resort)**.

What you do (optional but powerful):

- If your email supports it, switch from SMS codes to an authenticator app or passkeys.
- Save backup codes in a secure place.

This reduces SIM-swap risk and makes "code interception" harder.

Step 6: Run the Weekly 10-Minute Habit (This Is How You Stay Safe Long-Term)

Chapter 3 explains your weekly routine is simple: **review alerts → review transactions → do one improvement.**

Since you just had an MFA warning, your "one improvement" this week is:

- Email password reset + recovery cleanup + MFA upgrade.

Then you do the other two parts:

- Scan security alerts (email, bank, carrier, password manager, social).
- Review recent bank/credit transactions for anything unfamiliar.

Outcome (What Happens in This Case)

Because you followed the 80/20 baseline:

- The attacker **didn't get in** (you didn't approve the prompt).
- Your email password is now **unique and newly rotated**.
- Recovery settings and sessions are **cleaned up** so they can't "sneak back in."
- Your overall security improves without needing complicated tech skills.

"Do This Next Time" Summary (30 seconds)

1. Unexpected MFA prompt = treat as a warning sign.
2. Change your email password using your password manager.
3. Audit recovery + devices/sessions.
4. Keep the habit: alerts → transactions → one improvement.

Case Study (Chapter 3) — Meet Olivia Chen: The 80/20 Baseline in Action

Who Olivia Is

Olivia Chen is a 33-year-old small business owner who does everything from her phone—banking, invoicing, shopping, and social media. She's not "techy," but she's willing to follow simple steps if they actually work.

The Moment

At 8:41 p.m., Olivia is watching TV when her phone lights up:

"Your email sign-in code is: 593204"
She wasn't signing in anywhere.

Her first thought is panic: *"Is someone in my email right now?"*
This is exactly the kind of moment Chapter 3 prepares you for.

Step 1: Olivia Uses the "Top 5 Accounts" Lens (80/20 Thinking)

Instead of trying to secure everything, Olivia remembers Chapter 3's rule: focus on the accounts that matter most:

1. **Email** (password resets)
2. **Banking/credit cards** (money)
3. **Phone carrier** (SIM swaps)
4. **Password manager** (the vault)
5. **Primary social** (impersonation)

Because the code is for her **email**, she treats it as a "front door" alert.

Step 2: Olivia Follows the MFA Rule: "Approve Only When You Initiated It"

Olivia does **not** enter or share the code.
She treats an unexpected code as a warning sign that someone may already have her password and is trying to get past the second step.

Step 3: Olivia Fixes the Problem Fast Using a Password Manager

Olivia opens her password manager and does a "lockdown sprint":

1. Generates a **new strong password** for her email
2. Changes her email password immediately
3. Saves it to the vault

This breaks the attacker's attempt because the old password is now useless.

Step 4: Olivia Checks the Hidden Weak Spot: Recovery + Sessions

Next, Olivia secures the "back doors" that attackers love:

- **Recovery email/phone:** removes an old phone number she no longer uses
- **Devices/sessions:** signs out of anything unfamiliar
- **Backup codes:** stores them securely so she won't get locked out later

Now even if someone tries again, it's much harder for them to regain access.

Step 5: Olivia Strengthens MFA (Best Available Option)

Olivia checks her email security settings and upgrades MFA to the best option available (authenticator/passkeys if offered).
Then she makes a personal rule: **“If I didn’t initiate it, I don’t approve it.”**

Step 6: Olivia Runs the “Weekly 10-Minute Habit” to Prevent the Next Hit

Instead of stopping here, Olivia uses Chapter 3’s maintenance habit:

Alerts → Transactions → One Improvement

- Alerts: scans for any new security emails from bank/social/carrier
- Transactions: checks the last few days for small “test charges”
- One improvement: enables MFA on her primary social account next

This turns a scary moment into a long-term upgrade.

Outcome (What Olivia Learned)

Olivia didn’t need to be an expert. Her safety came from:

- prioritizing the Top 5 accounts,
- using a password manager for fast resets,
- treating unexpected MFA prompts as a real warning,
- and keeping security alive with a small weekly routine.

“Do This Next Time” Summary (30 seconds)

1. Unexpected MFA prompt = **don’t approve**
2. Secure **email first** (new password + MFA)
3. Check **recovery + sessions**

4. Weekly habit: **alerts → transactions → one improvement**

Case Study (Chapter 4): “The Toll Text Scam—Running the 5-Step AI Scam Check Workflow”

This case study follows Chapter 4’s exact approach: learn the **universal scam signals**, run the **5-Step AI Scam Check Workflow** (Pause → Sanitize → Red Flags/Risk Rating → Verification Steps → Verify + Decide), use **link safety without clicking**, and rely on **simple reply scripts** when needed.

The Situation

It’s mid-morning. You get a text from an unknown number:

“FINAL NOTICE: Unpaid tolls of $17.40. Pay within 30 minutes to avoid $500 fine. Pay now: [short link]”

This matches one of the common message scam categories Chapter 4 highlights (toll/ticket scams) and uses multiple universal signals at once.

Step 1 — PAUSE (Don’t Click, Don’t Reply)

Chapter 4 starts with a simple rule: your first move is not to tap. You **pause** to break the urgency spell.

What you do:

- You do **not** click the link.
- You do **not** reply “STOP” (replying can confirm your number is active).
- You take one breath and move to the workflow.

Step 2 — SANITIZE (Make It Safe to Ask AI)

Chapter 4's workflow emphasizes sanitizing before you use your AI assistant: remove/break links, remove identifiers, keep the core text.

Sanitized version you can paste:
"Text from unknown number: 'FINAL NOTICE: Unpaid tolls of $[AMOUNT]. Pay within 30 minutes to avoid $[FINE]. Pay now: [LINK_REMOVED].'"

Step 3 — ASK AI FOR RED FLAGS + A RISK RATING

Chapter 4 recommends asking AI to analyze patterns (red flags + risk rating), not to "prove" legitimacy.

Prompt (tool-agnostic):
"Analyze this sanitized text for common scam signals.

1. Risk rating (Low/Med/High)
2. The red flags you see
3. Why scammers use these tactics"

What the AI should notice (based on Chapter 4's universal signals):

- **Urgency** ("within 30 minutes")
- **Threat/pressure** ("$500 fine")
- **Suspicious link** (short link)
- **Identity confusion** (unknown number claiming authority)

With urgency + threat + link together, Chapter 4 says treat it as **high risk** and verify independently.

Step 4 — ASK AI FOR SAFE VERIFICATION STEPS (No Clicking)

This is the key pivot in Chapter 4: don't ask "is it real?"—ask how to verify safely without using the message's link or number.

Prompt:
“Assume this could be a scam. Give me safe steps to verify without clicking the link or calling any number in the text. Keep it short.”

Expected safe verification steps (aligned with Chapter 4 “Link Safety Without Clicking”):

- Use your **official toll account app** (if you have one) or type the official website yourself.
- Look up your state/regional toll agency’s official site using a trusted method (bookmark, typed URL, or known statement info).
- Check if you have any recent toll activity/violations **inside the official portal**.

Step 5 — VERIFY + DECIDE (Official Channel Only)

Now you verify using a channel **you** control (not the scam’s link).

What happens in this case study

You check your actual toll account / official agency portal: **no unpaid tolls**, no notices.

Decision:

- Delete the text
- Block the number
- Optionally report as spam/junk

This is exactly how Chapter 4 frames success: you didn’t “outsmart” the scam—your system prevented a rushed click.

If You *Must* Reply (Rare “Gray Area” Situations)

Chapter 4 includes simple scripts for boundary-setting. Most obvious scam texts deserve **no reply**, but if you ever need a script for a questionable message, use:

Safe reply options (copy/paste):

- “I don’t click links from texts. I’ll verify through the official site/app.”
- “I’ll contact support directly using official contact information.”
- If anyone asks for a code: “I don’t share verification codes.”

Quick Summary (The Chapter 4 “Do This Every Time” Loop)

1. **Pause** (don’t click)
2. **Sanitize** the message (remove links + identifiers)
3. Ask AI for **red flags + risk rating**
4. Ask AI for **verification steps** (no message links)
5. **Verify in the official app/site you access yourself**, then decide

Case Study (Chapter 4) — Meet Jamal Brooks: The “Toll Violation” Text Scam

Who Jamal Is

Jamal Brooks is a 29-year-old delivery driver who’s always on the move. He pays bills on his phone between stops, so when a message looks official and urgent, it’s tempting to “handle it fast” and keep going.

The Moment

At 11:26 a.m., Jamal gets a text from an unknown number:

“FINAL NOTICE: Unpaid tolls of $17.40. Pay within 30 minutes to avoid a $500 fine. Pay now: [LINK]”

His first thought: *“Did I miss a toll?”*
His second thought: *“I can’t deal with a $500 fine—let me pay this real quick.”*

Chapter 4 exists for this exact moment: **a high-pressure message trying to make you click before you think.**

Step 1 — PAUSE (Don’t Click, Don’t Reply)

Jamal remembers the Chapter 4 rule: the first win is simply not tapping.

- He does **not** click the link.
- He does **not** reply “STOP” (replying can confirm his number is active).
- He takes one breath and moves to the process.

Step 2 — SANITIZE (Make It Safe to Ask an AI Assistant)

Chapter 4's workflow uses AI as a helper, but safely. Jamal removes the link and any identifiers.

Sanitized version (safe to paste):
"Text from unknown number: 'FINAL NOTICE: Unpaid tolls of $[AMOUNT]. Pay within 30 minutes to avoid $[FINE]. Pay now: [LINK_REMOVED].'"

Step 3 — ASK AI FOR RED FLAGS + A RISK RATING

Jamal uses an AI assistant to spot patterns and name the danger signals.

Prompt:
"Analyze this sanitized text for common scam signals.

1. Risk rating (Low/Med/High)
2. Top red flags
3. Why these tactics work on people"

What the AI points out (Chapter 4 universal signals):

- **Urgency** ("within 30 minutes")
- **Threat/pressure** ("$500 fine")
- **Suspicious link** (short link)
- **Authority impersonation** (toll agency vibe without proof)

That combination typically equals **High Risk**.

Step 4 — ASK AI FOR SAFE VERIFICATION STEPS (No Clicking)

Chapter 4 teaches the best question isn't "Is it real?"
It's: **"How do I verify safely without using their link?"**

Prompt:
“Give me 3 safe ways to verify this without clicking any link or calling any number in the message.”

Safe verification steps Jamal gets:

1. Open the official toll account/app (if he has one) and check for notices.
2. Type the official toll agency website manually (or use a saved bookmark) and look up account/plate notices.
3. If needed, find the official contact number from the official website (typed manually) and ask if any notice exists.

Step 5 — VERIFY + DECIDE (Official Channel Only)

Jamal verifies through channels **he controls**, not the message.

- He checks the official toll portal (typed in manually).
- No notices. No unpaid tolls. No fines.

Decision:

- Delete the message
- Block the number
- Report as junk/spam if his phone allows

What Jamal Learned (Chapter 4 in One Line)

He didn’t need to know every scam type. He just needed a repeatable system:
Pause → Sanitize → Ask AI for red flags → Ask AI how to verify → Verify officially → Decide.

Optional “Safe Reply” Scripts (If You Ever Need One)

Most obvious scam texts don’t deserve a reply, but if Jamal ever needed a script, Chapter 4’s style is:

- “I don’t click links from texts. I’ll verify through the official site/app.”
- “I don’t handle account issues by text. I’ll contact support directly.”
- If asked for a code: “I don’t share verification codes.”

If you want, I can create **two more character-based Chapter 4 case studies** for your workbook:

1. **“Package Delivery Problem” text** (link trap)
2. **“Subscription Renewal Invoice” email** (refund scam bait)

Case Study (Chapter 5): “The ‘Bank Fraud Department’ Call—How to Beat Spoofing and Deepfakes”

This case study follows Chapter 5’s playbook: **caller ID can’t be trusted**, recognize the **common phone scam scripts**, use the beginner defense for **deepfake voice** (behavior over sound), apply the **Hang Up + Call Back method**, use a **family code word**, and know what to do **if you already shared info**.

The Situation

It’s 2:18 p.m. Your phone rings.

Caller ID: *Your bank’s name* (and it even shows the bank’s real customer service number).
A calm voice says:

“Hi, this is the fraud department. We detected suspicious activity and need to secure your account immediately. I’m going to send you a code—read it to me so I can verify I’m speaking to the account owner.”

Your heart rate jumps. It sounds official. The caller knows your name and the last 4 digits of a card. Chapter 5 warns this exact setup is common because **caller ID can be spoofed** and scammers often impersonate banks using familiar numbers.

Step 1 — Treat Caller ID as a Clue, Not Proof

Chapter 5’s core idea: **Caller ID can be faked**, so you judge the call by behavior and requests, not the label on your screen.

Red flag right away: They want a **verification code** on an incoming call.

Step 2 — Spot the Script (Common Phone Scam Pattern)

Chapter 5 explains the common “bank fraud” script:

- “There’s suspicious activity”
- “We need to verify you”
- “Read the code / confirm details”
- sometimes “move money to a safe account”

This is designed to keep you on the line until you comply.

Step 3 — Use the Beginner Deepfake Defense (Behavior Over Sound)

Chapter 5 notes that deepfakes can sound convincing, but you don’t need to analyze audio—focus on behavior:

- **Urgency**
- **Pressure**
- **Refusal to let you verify**
- **Keeping you on the line**

Rule: urgent + “don’t verify” = hostile until proven otherwise.

Step 4 — The Hang Up + Call Back Method (Exact Steps)

This is the chapter’s strongest move: **you take control of the channel**.

What you say (calm script)

“Thanks. I’m going to hang up and call back through the official number on my card/app to verify.”

What you do next

1. **Hang up.**
2. **Open your bank’s official app** (or call the number on the back of your card).
3. Ask:
    - “Do you see any alerts on my account?”
    - “Did your fraud department just call me?”
    - “Are there any holds, transfers, or new payees?”

What happens in this case study:
Your bank confirms: **They did not call you.** There is **no case**, and the “fraud rep” was fake.

That’s the win: you broke the scammer’s controlled environment by calling back through a trusted channel.

Step 5 — Add a Family Safety Layer (Code Word)

Chapter 5 also teaches a family verification system—especially for “family emergency” calls and voice impersonation.

Example: You and your household agree on a simple code word.
If anyone calls claiming to be a family member in trouble and asks for money, the first question is:

“What’s the code word?”

If they can’t answer, you **hang up and call back** a known number.

Step 6 — If You Already Shared Info (Quick Containment)

Chapter 5 includes a “don’t panic—act” section: if you already gave something away, your goal is to **stop the bleeding**.

If you **read a code** or gave info:

1. Call your bank using the number on your card and report suspected fraud.
2. Change your **email password** and review sessions (email is often the master key).
3. Change banking passwords and enable/confirm MFA.
4. If you notice loss of cell service, contact your carrier (SIM swap risk).

(Then jump to the full emergency steps in Chapter 11 when needed.)

Quick “Do This Next Time” Summary

1. Caller ID can be spoofed—don’t trust it as proof.
2. Never share verification codes on an incoming call.
3. Use **Hang Up + Call Back** via official numbers you find yourself.
4. Use a **family code word** for urgent money requests.

Case Study (Chapter 5) — Meet Elaine Morris: The “Grandson Emergency” Call (Spoofing + Deepfake Pressure)

Who Elaine Is

Elaine Morris is a 67-year-old grandmother who loves her family and answers her phone because she worries something could be wrong. She’s careful with money, but she’s never had someone try to weaponize emotion against her—until today.

The Moment

At 9:12 a.m., Elaine gets a call from an unknown number. The voice sounds shaky and desperate:

“Grandma… it’s me. I’m in trouble. Please don’t tell Mom. I need help right now.”

Then a second voice comes on—calm, firm, authoritative:

“Ma’am, I’m an officer/attorney. Your grandson was involved in an incident. If you don’t act immediately, this gets worse. We need you to send money today.”

Elaine’s heart pounds. Her mind jumps to the worst-case scenario.

Chapter 5 explains that scammers use **emotional manipulation** and **urgency** to keep you on the line—and with deepfake audio, the voice can sound “real” even when it’s not.

Step 1 — Remember the Rule: Caller ID + Voice Are Not Proof

Chapter 5 teaches a key reality: **caller ID can be spoofed**, and even a familiar voice can be faked or manipulated. Elaine doesn't need to "analyze the voice." She needs to control the channel.

Elaine's first thought becomes her first action:

"I'm going to verify."

Step 2 — Spot the Script (Phone Scam Pattern)

Elaine notices three classic pressure moves Chapter 5 warns about:

- **Urgency:** "right now," "today," "don't hang up"
- **Secrecy:** "don't tell his parents"
- **Authority:** "officer/attorney" insisting on immediate action

This is the moment Chapter 5 wants readers to recognize:
urgent + "don't verify" = hostile until proven otherwise.

Step 3 — Use the Chapter 5 Countermove: Hang Up + Call Back

Elaine uses the exact chapter method: **hang up and call back using a number she already trusts**.

She says calmly:

"I'm going to hang up and call my family directly. If this is real, we will handle it through official channels."

Then she **hangs up**.

This breaks the scammer's power, because the scam only works while they control the conversation.

Step 4 — Add the Family Verification System (Code Word)

Chapter 5 recommends a family verification system: **code word + call-back rule + no money on the first call**.

Elaine calls her daughter first, then calls her grandson using a number already saved in her contacts.

She uses the family verification question/code word:

"What's our family code word?"

Outcome: the real grandson answers normally and is safe—he has no idea what she's talking about.

Now Elaine knows with certainty: it was a scam.

Step 5 — If They Call Back (What Elaine Does Next)

The scammers call again. Elaine follows Chapter 5 guidance:

- She does **not** argue.
- She does **not** explain.
- She **blocks** the number and reports it as spam if possible.

She also warns her family:

"If anyone gets a call claiming someone is in trouble and asking for money, hang up and call back. No exceptions."

This prevents follow-on targeting.

Step 6 — “What If I Had Already Paid?” (Chapter 5 Safety Net)

Chapter 5 includes an important point: if you already shared information or sent money, **don’t freeze—act quickly** and move into the emergency response flow (Chapter 11).

If Elaine had paid, her next actions would be:

1. Call her bank/card using an official number and report fraud immediately
2. Document the details (time, number, requested payment method)
3. Secure key accounts (email first, then banking)

What Elaine Learned (Chapter 5 in One Line)

You don’t beat phone scams by debating—you beat them by changing the channel. Hang up, call back, verify.

Case Study (Chapter 6): “The ‘Friend’ DM + Marketplace Payment Screenshot Scam”

This case study follows Chapter 6’s exact focus: **account takeover traps**, **impersonation scams**, **marketplace traps**, and the **hard safety rules** (no codes, no off-platform payments, no remote access, no verification screenshots), plus using AI the right way to draft calm boundary messages and verification steps.

The Situation

You get a DM on social media from someone who looks like your friend “Megan.”

DM:
“Hey! My old account got locked. Can you help me get back in? I’m sending you a link—just log in and confirm it’s you.”

A minute later, you also get a message from a “buyer” on a marketplace listing you posted:

Buyer:
“I sent payment—see screenshot. Can you ship it today? It’ll clear once you send tracking.”

This is exactly the kind of “friendly stranger / social trust” setup Chapter 6 warns about: scammers borrow trust from relationships and platforms to get you to click, share codes, or send items/money fast.

Step 1 — Identify the Two Scam Patterns (Chapter 6 Map)

A) Account takeover trap ("Is this you?" / fake login link)

- A link arrives in a DM.
- It tries to push you to log in "to help."
- The goal is your **account** (steal your password/codes).

B) Marketplace trap (fake payment proof)

- They show a "payment screenshot."
- They pressure you to ship before money is confirmed.
- The goal is your **stuff** (and sometimes more info later).

Step 2 — Apply the Chapter 6 Hard Rules (Non-Negotiables)

Chapter 6 ends with rules that block most of these scams immediately. Use them like a checklist:

- **No codes** (never share login/MFA codes—ever).
- **No off-platform payments** (only use official checkout/buyer protection).
- **No remote access** (never install "support" tools or screen share).
- **No verification screenshots** (they can leak info and help takeovers).

So your immediate decision is easy: **don't click the DM link** and **don't ship** based on a screenshot.

Step 3 — Use "Two-Channel Confirmation" to Verify the Friend

Chapter 6 emphasizes verifying identities through a channel you control—especially when trust is being borrowed.

What you do:

1. Don't reply to the DM link request.

2. Text/call Megan using a number you already have (or message her original verified account).
3. Ask one simple question only the real person would know (or use your family/friend code word if you have one).

Outcome in this case study:
Megan replies: “That’s not me. I’m locked out and someone is cloning accounts.”

Now you know it’s impersonation, not a misunderstanding.

Step 4 — Use AI the Chapter 6 Way: Draft Boundaries + Safe Next Steps

Chapter 6 supports using AI to **analyze manipulation patterns** and **draft refusal/boundary messages**—not to “detect truth,” but to keep you calm and consistent.

Safe AI prompt (sanitized)

“Draft a calm message that refuses to click links or share codes and tells the person I will verify through official channels. Keep it short and firm.”

AI-generated boundary script you can send:

- “I don’t click login links from DMs or share codes. If this is real, contact platform support through the official app.”

Then, for the marketplace buyer:

Safe AI prompt (sanitized):
“Draft a short seller message: I only ship after payment is confirmed inside the platform. No screenshots accepted.”

Seller script:

- “Thanks. I only accept payment through the platform’s official checkout. I’ll ship after the payment shows as completed in my account.”

Step 5 — Marketplace Verification (Platform-Only)

Chapter 6 warns that screenshots are easy to fake and off-platform pressure is a classic trap.

What you do:

1. Ignore the screenshot.
2. Open the marketplace app and check **your actual payment status**.
3. Only proceed if it shows “Paid/Completed” inside the platform.
4. If they insist on Venmo/CashApp/Zelle “to avoid fees,” you decline (that’s a red flag and removes protections).

Outcome in this case study:
No payment exists in the platform. The buyer pushes harder and wants you to ship anyway. You block/report and move on.

Step 6 — Recovery Actions (Chapter 6 Clean-Up)

Chapter 6 includes “recovery” steps when links get clicked or accounts are threatened.

If you clicked the DM link (even once), do this:

- Change your social password (unique)
- Turn on/confirm MFA
- Review logged-in devices/sessions
- Warn close contacts: “If you get a weird link from me, don’t click.”

And report:

- Report the fake profile/account to the platform
- Screenshot the fake profile (for reference) before it disappears

---

Quick Summary (What the Reader Learns From Chapter 6)

- Social scams work by borrowing trust—**verify identities outside the DM.**
- Marketplace scams use pressure + screenshots—**only trust what you can confirm inside the official platform.**
- The hard rules do the heavy lifting: **no codes, no off-platform payments, no remote access, no verification screenshots.**

Case Study (Chapter 6) — Meet Sofia Alvarez: The “Is This You?” DM + Fake Marketplace Buyer

Who Sofia Is

Sofia Alvarez is a 26-year-old teacher who uses social media to stay in touch with friends and a marketplace app to sell extra household items. She’s careful, but she’s also polite—and scammers love polite people because they hesitate to say “no.”

The Moment

Sofia gets two messages within the same hour:

DM from “Friend” (looks like her cousin):

“Hey Sofia! Is this you? I think your account got hacked. Check this link asap: [LINK]”

Marketplace message from a buyer:

“I sent payment. Here’s the screenshot. Can you ship today? I’m in a hurry.”

Chapter 6 warns that social and marketplace scams succeed because they borrow **trust** (friends/community) and create **speed pressure** to bypass safety steps.

Step 1 — Sofia Identifies the Scam Categories (Chapter 6 Map)

Chapter 6 lays out several common patterns. Sofia recognizes both immediately:

A) Account Takeover Pattern ("Is this you?" link)

This is a classic **account takeover trap**: a message tries to lure you into clicking a login link or entering credentials.

B) Marketplace Trap (Fake payment proof)

The buyer uses a screenshot to create false confidence and rush shipping before money is confirmed.

Sofia remembers: **screenshots are not proof**—only the platform's official payment status is proof.

Step 2 — Sofia Uses the Chapter 6 "Hard Rules" (No Negotiation)

Chapter 6 gives rules that block most of these scams instantly:

- **No codes** (never share them)
- **No off-platform payments** (platform checkout only)
- **No remote access** (never install "support" tools)
- **No verification screenshots** (don't send screenshots of codes/identity/confirmation pages)

Sofia applies them:

- She does **not** click the DM link.
- She does **not** accept payment "proof" by screenshot.
- She does **not** ship anything until she sees confirmed payment inside the platform.

Step 3 — Sofia Verifies the "Friend" with Two-Channel Confirmation

Chapter 6 warns that impersonation scams are common (fake profiles of friends, schools, local groups). The fix is **verification through a channel you control**.

Sofia does this:

1. She doesn't respond to the DM link.
2. She texts her cousin using the number already saved in her phone:
    - "Did you just message me with a link?"
3. She asks a quick confirmation question only the real cousin would know.

Outcome: Her cousin replies, "No—my account got hacked too."

Now Sofia knows the DM was an impersonation attempt.

Step 4 — Sofia Uses AI the Right Way (Draft a Calm Boundary Message)

Chapter 6 supports using AI to **draft boundaries/refusal messages** and **analyze manipulation patterns**, not to "detect truth."

Sofia asks her AI assistant:

Prompt (safe and tool-agnostic):
"Write a short message that refuses to click login links or share codes and says I'll verify through the official app. Keep it calm and under 40 words."

Sofia sends:

"I don't click login links or share codes in DMs. If there's an issue, I'll verify through the official app/settings."

Then she blocks and reports the impersonator.

Step 5 — Sofia Verifies Marketplace Payment the Only Way That Counts

Chapter 6 warns about marketplace traps: fake payment confirmations, deposit pressure, courier scams.

Sofia checks:

- Her marketplace **order status** inside the app
- Her account balance/transactions inside the platform

Outcome: No payment is shown as completed.

The buyer pressures her:

“It’s pending. Just ship and it’ll clear.”

Sofia remembers Chapter 6’s hard rule: **platform-only payments** and **no shipping without confirmed payment**.

She replies (short and firm):

“I only ship after payment is confirmed inside the platform. Thanks.”

The buyer gets angry and tries to push off-platform payment methods.

Sofia blocks and reports.

Step 6 — Sofia Does the Chapter 6 “Recovery” Step (Just in Case)

Chapter 6 includes recovery actions if you clicked a link or suspect takeover attempts.

Sofia takes 10 minutes to:

- Change her social password to a strong unique one
- Turn on MFA
- Review sessions/devices

- Send a short note to close contacts:
  “If you get a weird link from me, don’t click—it’s not me.”

What Sofia Learned (Chapter 6 in One Line)

Social scams win by borrowing trust and creating speed. Your defense is simple: verify through a channel you control and follow the hard rules.

Case Study (Chapter 7): “Email Takeover Attempt—Lock Down the Master Key Before It Spreads”

This case study follows Chapter 7’s core message: **email is the master key** (password resets + sensitive info), and the practical Email Lockdown steps: **turn on MFA, audit recovery options, review sessions/devices, check forwarding/rules, and revoke third-party access**—plus the “Unexpected MFA Prompt” warning sign.

The Situation

You wake up to two emails that make your stomach drop:

1. **“New sign-in to your email account”**
2. **“Password reset requested for your shopping account”**

A minute later, you get an **unexpected MFA code** text for your email account—even though you didn’t try to log in.

Chapter 7 explains why this is dangerous: if someone gets into your email, they can reset passwords for banking, shopping, and other accounts—often before you notice.

Step 1 — Recognize the Real Threat: Email Is the Master Key

Before you start changing random passwords, you follow Chapter 7’s mindset:

- This isn’t “just an email issue.”
- Email controls password resets and receives security alerts.
- Attackers may also use forwarding rules to secretly watch your inbox.

So you treat this as a “master key” emergency and prioritize email first.

Step 2 — Apply the “Unexpected MFA Prompt” Rule

Chapter 7 teaches that unexpected MFA prompts aren’t noise—they’re an alarm bell that someone may already have your password and is trying to get in.

What you do immediately:

- Do **not** approve any prompt.
- Do **not** share the code with anyone.
- Move straight to lockdown actions.

Step 3 — Email Lockdown: The 5-Step Chapter 7 Fix

A) Turn on / confirm MFA

If MFA is off, turn it on now. If it’s on, confirm it’s using your correct method and that no unfamiliar methods are added. Chapter 7 recommends using MFA to block password-only attacks.

B) Recovery audit (hidden back door)

Go to your email account’s security/recovery settings:

- Remove old recovery phone numbers and recovery emails
- Replace anything you don’t recognize
  Chapter 7 warns that neglected recovery details can become a back door for attackers.

C) Sessions/devices cleanup (kick them out)

Open the “Devices” or “Where you’re signed in” screen:

- Sign out of any device you don’t recognize

- Use “Sign out of all devices” if available, then sign back in only on trusted devices
  Chapter 7 emphasizes reviewing sessions/devices to remove silent access.

D) Forwarding + rules check (quiet attacker trick)

Check:

- Forwarding addresses
- Filters/rules that auto-delete, auto-archive, or forward “security” and “bank” emails
  Chapter 7 notes attackers love these because most people never check them.

E) Revoke third-party app access

Review connected apps / “Sign in with…” permissions:

- Remove anything you don’t recognize or no longer use
  Chapter 7 calls out third-party access as an overlooked pathway into your email.

Step 4 — Stop the Cascade: Secure the Accounts Email Can Reset

Now that the master key is secured, you prevent the “domino effect” Chapter 7 warns about:

Priority list (fast):

1. Banking / credit card logins
2. Shopping accounts with stored cards
3. Payment apps
4. Primary social accounts

Change passwords to unique ones (ideally stored in a password manager), and enable MFA where available—so an email takeover can’t easily spread.

Step 5 — Verify What Happened (Without Panic)

Chapter 7's approach is practical, not paranoid:

- Check your email "Sent" folder for messages you didn't send
- Check security activity logs if available
- Look for password reset emails you didn't request

If you find suspicious resets, you reset those accounts immediately and keep notes for later follow-up.

Outcome (What Happens in This Case Study)

Because you treated email as the master key and used the Chapter 7 checklist:

- Any attacker sessions are kicked out
- Recovery back doors are removed
- Forwarding/rules traps are cleared
- Third-party access paths are closed
- The takeover doesn't spread to banking or other accounts

That's a win: you shut down the "email → reset everything" chain quickly.

Quick "Do This Next Time" Summary

1. Email threat = master key threat.
2. Unexpected MFA prompt = treat as an active attack.
3. Lock down: MFA → recovery → sessions → rules → third-party apps.
4. Then secure top accounts that email can reset.

Case Study (Chapter 7) — Meet Derek Walsh: The Email Master Key Lockdown

Who Derek Is

Derek Walsh is a 41-year-old operations manager who keeps his life organized through email—bank alerts, receipts, password resets, kids' school updates, and work logins. He's careful, but he's never checked email forwarding rules before (most people haven't).

The Moment

On a Tuesday morning, Derek notices something strange:

- A "Password reset requested" email for an online retailer he uses
- A security alert: **"New sign-in detected"** to his email account
- Then a second alert: **"A forwarding address was added"**

Derek's first instinct is to immediately change a bunch of passwords. But Chapter 7 teaches a more effective rule:

Email is the master key. Secure email first, or attackers will keep resetting everything.

Step 1 — Derek Names the Real Risk: Email Can Reset Everything

Derek pauses and recognizes what Chapter 7 explains:

- If someone controls email, they can trigger password resets for banks, shopping, social, and more.

- They can also hide by using forwarding and rules to quietly watch and delete security emails.

So Derek's plan is not "change everything." It's **lock down email first**.

Step 2 — Derek Runs the Chapter 7 Email Lockdown Steps (In Order)

A) Turn on / confirm MFA (the main lock)

Derek checks email security settings and confirms MFA is on.
If it weren't, this would be his first move—because it blocks password-only takeovers.

B) Recovery audit (close the back door)

He checks:

- recovery phone numbers
- recovery email addresses
- security questions (if present)

He removes an old phone number from years ago. That old number could have been used to regain access.

C) Sessions/devices cleanup (kick them out)

Derek opens "Where you're signed in" and sees a device he doesn't recognize.
He uses "sign out of all devices," then signs back in only on his trusted phone and laptop.

D) Forwarding + filters/rules review (the sneaky attacker trick)

Now Derek checks:

- Forwarding addresses
- Rules/filters that auto-archive, auto-delete, or forward messages

He finds a rule that forwards anything with “security,” “password,” and “bank” to a strange address, then archives it.
This is exactly how attackers stay invisible—Derek deletes it immediately.

E) Third-party app access (quiet long-term access)

Derek reviews connected apps and sees a “free coupon finder” tool he used once.
It has permission to read his email. He revokes access.

Step 3 — Derek Applies the “Unexpected MFA Prompt” Rule

He remembers Chapter 7’s warning:
If you get an MFA prompt you didn’t initiate, treat it like an active attack.

Derek didn’t approve anything. He changed his password, signed out sessions, and removed hidden rules. That’s why the attacker lost access.

Step 4 — Derek Stops the Cascade (Secure the Accounts Email Can Reset)

Now Derek secures the most important accounts that could have been targeted next:

1. Banking and credit card logins
2. Shopping accounts with stored payment methods
3. Any payment apps
4. Primary social account

He changes passwords to unique ones (stored in a password manager) and turns on MFA where available.

Step 5 — Derek Prevents a Repeat (A 10-Minute Weekly Habit)

To keep it from happening again, Derek adopts a simple habit:

- Check security alerts
- Check transactions
- Make one improvement (one account per week)

This keeps him ahead without becoming obsessive.

Outcome (What Derek Learned)

Derek didn't "fight the hacker." He simply locked down the master key using a repeatable checklist:

- MFA
- recovery audit
- sessions cleanup
- rules/forwarding check
- third-party access review

Once email was secure, the rest became manageable.

Chapter 7 in One Line

Secure email first, because email is where attackers go to reset everything else.

Case Study (Chapter 8): “My Phone Lost Service—Is This a SIM Swap?”

This case study follows Chapter 8’s exact focus: **phone hardening basics** (updates, screen lock, permissions), **SIM swap protection** (carrier PIN + port-out/SIM-change lock), **fake popups/tech support traps**, **public Wi-Fi rules**, and **home Wi-Fi basics**—with the chapter’s key “act fast” moment: **sudden loss of cell service can be a SIM-swap emergency**.

The Situation

You’re running errands when your phone suddenly shows **“No Service.”** You toggle airplane mode—still nothing. A minute later, you get an email notification on your smartwatch:

“Your bank password was reset.”

Then a text arrives on your spouse’s phone:

“Your number was transferred to a new device.”

Chapter 8 explains why this combination matters: if someone hijacks your phone number, they can intercept codes and reset accounts quickly.

Step 1 — Treat “No Service” as a Potential SIM Swap (Don’t Wait It Out)

Chapter 8 teaches a simple rule: if your phone loses service unexpectedly in an area where it usually works, **treat it as urgent—not an inconvenience**.

What you do immediately:

- Don’t keep troubleshooting for 30 minutes.
- Don’t rely on texts coming to your phone (they may be going to the attacker now).
- Move straight to verification and containment.

Step 2 — Switch Channels: Call Your Carrier From Another Phone

Because your number may be compromised, you borrow a phone (spouse/friend) or use a landline.

What you say (simple script based on Chapter 8):

“I believe my SIM may have been fraudulently swapped. Please **lock my account**, **reverse any SIM/port-out changes**, and require my **account PIN** for any future changes.”

Chapter 8 emphasizes adding a **carrier PIN/passcode** and requesting a **port-out/SIM-change lock** to prevent this exact scenario.

Outcome in this case study:
Carrier confirms: a SIM change was requested 10 minutes ago. They **freeze the line**, start reversal, and add extra protections.

Step 3 — Secure the Accounts Most at Risk (Email + Banking)

Chapter 8 connects directly to earlier chapters: if the attacker is trying to use your number to get codes, you must lock down the “master key” accounts fast.

Priority actions (10 minutes):

1. **Secure email** (change password + confirm MFA + sign out sessions).
2. **Secure banking** (change password, check transfers, enable alerts).
3. **Secure payment apps** (anything that can send money quickly).

If you can’t access accounts on cellular, use trusted Wi-Fi—but follow Chapter 8’s public Wi-Fi rules (next step).

Step 4 — Use Safe Network Rules (Public Wi-Fi vs Cellular)

Chapter 8 warns that public Wi-Fi can add risk, especially for sensitive logins.

Safe choice hierarchy:

- Best: cellular data (but your line may be down)
- Next best: a trusted/private Wi-Fi network
- Last resort: public Wi-Fi (avoid banking resets if possible)

What you do in this case study:

- You use a trusted hotspot (spouse’s phone) or a known Wi-Fi network,
- You avoid clicking links in emails/texts and instead open official apps directly.

Step 5 — Check for the “Tech Support” Trap (If a Popup Appears)

While you’re searching for carrier support, a popup appears:

“Virus detected! Call Apple/Microsoft Support now!”

Chapter 8 explains fake popups are designed to push you to call a scam number or install remote access tools.

What you do (Chapter 8 steps):

1. Do **not** call the number.
2. Force-close the browser/app (restart if needed).

3. Update and scan later using trusted tools.

Step 6 — Lock In Preventive Protections (After You Stabilize)

Once your carrier restores service and your accounts are safe, you apply Chapter 8's prevention steps so it's harder next time:

Phone hardening basics

- Turn on automatic OS/app updates
- Use a strong screen lock (6+ digit PIN + biometrics)
- Review app permissions and remove sketchy apps

SIM swap protections (do this even if you "think you already did")

- Confirm your carrier **PIN/passcode** is active
- Confirm **port-out/SIM-change lock** is enabled
- Ask what alerts exist for SIM/port requests

Home Wi-Fi basics (quick win)

- Change router admin password
- Enable firmware updates if available
- Use a guest network for visitors/IoT devices

Outcome (What the Reader Learns)

In this case study, you didn't "hack back." You followed the Chapter 8 playbook:

- You treated loss of service as a warning sign
- You switched channels and contacted the carrier safely
- You secured email/banking quickly
- You avoided popup traps and unsafe links
- You hardened phone + carrier + Wi-Fi afterward so it's less likely again

Quick “Do This Next Time” Summary

1. Sudden **No Service** = possible SIM swap. Act fast.
2. Call carrier from another phone; lock/reverse SIM change; add PIN + port lock.
3. Secure email + banking + payment apps immediately.
4. Don’t call popup numbers; close and verify via official support.

Case Study (Chapter 8) — Meet Kevin Ramirez: “No Service” + Codes Start Hitting

Who Kevin Is

Kevin Ramirez is a 37-year-old dad who runs errands, pays bills on his phone, and uses text codes for logins all the time. He’s not paranoid—he just wants life to work.

The Moment

Kevin is in a grocery store parking lot when his phone suddenly flips to **“No Service.”**
He assumes it’s a coverage issue—until two things happen:

1. His wife’s phone gets a text: **“Your number transfer request is processing.”**
2. Kevin’s email inbox (on Wi-Fi) shows: **“Password reset requested for your bank.”**

This is the Chapter 8 scenario: **a phone-number attack may be in progress** (SIM swap / port-out), and waiting it out can cost real money.

Step 1 — Kevin Treats “No Service” as a SIM Swap Warning (Don’t Wait)

Instead of rebooting his phone five times, Kevin uses the Chapter 8 rule: **Unexpected loss of service = verify immediately.**

He stops troubleshooting and switches into action mode.

Step 2 — Kevin Changes Channels: Calls the Carrier From Another Phone

Because Kevin's number may already be compromised, he borrows his wife's phone and calls the carrier using a trusted source (carrier app/website/statement contact).

What Kevin says (simple script):

"My phone suddenly lost service and I suspect SIM-swap or port-out fraud. Please **lock my account**, **stop any number transfer**, and **reverse any SIM/port changes**. Add a **carrier PIN** and a **port-out/SIM-change lock** so no changes happen without my PIN."

Outcome: The carrier confirms there was a change request and freezes the account while they reverse it.

Step 3 — Kevin Secures the Accounts That a SIM Swap Can Break Into

Chapter 8 connects to the "Top 5" idea: if someone steals your phone number, they can intercept codes and reset accounts.

Kevin's priority list:

1. **Email** (master key)
2. **Banking and payment apps**
3. **Password manager**
4. **Primary social**

What Kevin does next (10 minutes):

- Changes email password and checks logged-in sessions
- Confirms MFA is still set to his device/app (not an unknown number)
- Changes bank password and checks for transfers
- Turns on or confirms transaction/login alerts

Step 4 — Kevin Avoids the Tech Support Trap (Popups + “Call Now”)

While searching carrier info, Kevin gets a scary browser popup:

“Virus detected! Call support now!”

Chapter 8 warns: fake popups try to get you to call a scam number or install remote access tools.

Kevin follows the safe response:

- **Does not call** the number
- **Closes the browser/app**
- Plans to update and scan later using trusted tools

Step 5 — Kevin Uses Safe Network Habits While He Recovers

Kevin is tempted to use the coffee shop Wi-Fi next door. Chapter 8’s simple rule:

- Prefer trusted networks and official apps
- Avoid sensitive logins on public Wi-Fi when possible

So Kevin uses his wife’s hotspot and official apps to finish securing accounts.

Step 6 — Kevin “Hardens” the Phone for Next Time (Prevention Steps)

After service is restored, Kevin spends 20 minutes making future attacks harder:

Phone hardening

- Enables automatic OS/app updates
- Sets a strong screen lock (6+ digit PIN + biometrics)
- Reviews app permissions and deletes unused apps

Carrier protection

- Confirms carrier PIN is on file
- Confirms port-out/SIM-change lock is enabled
- Turns on carrier alerts for account changes (if available)

Home Wi-Fi quick check

- Changes router admin password
- Enables firmware updates
- Uses a guest network for smart devices

Outcome (What Kevin Learned)

Kevin didn't need technical skill—he needed speed and the right order:

- **No Service → call carrier from another phone**
- **Secure email + bank immediately**
- **Avoid popups and public Wi-Fi risks**
- **Lock in carrier protections after**

Chapter 8 in One Line

If your phone suddenly loses service, don't wait—verify with your carrier and secure email/banking fast.

Case Study (Chapter 9): “The Subscription Renewal Email—How to Protect Money, Set Alerts, and Dispute Fast”

This case study follows Chapter 9’s exact focus: **debit vs. credit (practical reality)**, using a **Safer Payment Ladder**, turning on the **alerts that matter**, recognizing the **biggest money scam patterns** (subscription/invoice and refund-style pressure), and knowing **how to dispute fast** with the right evidence and calm scripts.

The Situation

You open your email and see:

Subject: “Your Antivirus Subscription Renewed — $399.99”
Body: “If you did not authorize this renewal, call support immediately at 1-800-XXX-XXXX to cancel.”

You don’t remember buying this service. The email is designed to trigger panic—*“I need to cancel right now.”* Chapter 9 explains that scams often target your money using high-pressure “invoice/subscription” tactics and fast pathways to payment.

Step 1 — Use the Safer Payment Ladder Mindset (Before Anything Else)

Chapter 9 teaches that **how you pay** changes the damage:

- **Debit** pulls from your real checking money immediately (faster pain).

- **Credit** usually gives stronger dispute leverage because it's the issuer's money first.

In this case study:
You check and realize the email is trying to push you to call a number and potentially pay/"refund" something. You remind yourself: *If money moves, I want it moving on the safest rung possible—and I want proof before I act.*

Step 2 — Verify the Charge Inside Official Channels (Not the Email)

Chapter 9 is clear: don't let a message choose the channel. You verify through:

- your bank/credit card official app,
- your official account dashboards,
- trusted contact info (not the email).

What you do (3 minutes):

1. Open your **credit card app** (or bank app).
2. Search for a charge around **$399.99**.
3. Check your **recent transactions** and pending charges.

Outcome A (common scam outcome)

There is **no charge**. This email is bait to make you call a scam "support" line.

Decision: delete/report spam and move on.

Outcome B (scarier outcome)

You *do* see a pending charge you don't recognize. Now you shift into "dispute fast" mode.

Step 3 — Turn On the Alerts That Matter (So You Catch This Earlier Next Time)

Chapter 9 recommends setting alerts that actually help you detect fraud quickly without drowning in noise.

Alerts to enable (quick win):

- Online/card-not-present purchases
- ATM withdrawals
- New device/login alerts
- New payees (if available)
- Outgoing transfers (especially instant payments)

In this case:
You realize you never turned on online purchase alerts. You enable them immediately so a future “mystery renewal” triggers an alert right when it happens.

Step 4 — Recognize the Scam Pivot: The Refund Trap (What They Want Next)

Chapter 9 describes “refund scams” where the scammer claims they refunded too much and pressures you to send money back via irreversible methods.

If you call the number in the email, the script often becomes:

- “We can cancel it, but we need you to install a remote tool”
- “Oops, we refunded $4,000 instead of $400”
- “Send the difference back via wire/crypto/gift cards”

Chapter 9 rule:
Any push toward **gift cards/crypto/wire/instant transfer** is a loud warning sign.

So you do **not** call that number.

Step 5 — Dispute Fast (What to Save + What to Say)

Chapter 9 provides a practical dispute approach: gather simple evidence, contact the issuer using official channels, and log case numbers.

What you save (2 minutes)

- Screenshot of the email subject + sender (don't click links)
- Screenshot of the transaction in your bank/card app (amount/date/merchant)
- Notes: date/time you noticed it

What you do next (5–10 minutes)

Call the number on the back of your card or use secure in-app chat and say:

Dispute script (simple and effective):

"I'm calling to report a suspected fraudulent transaction. The charge is $[amount] on [date] to [merchant]. I did not authorize it and did not receive goods or services. Please open a dispute, block further charges from this merchant, and give me the case number."

You write down the case number and keep it in a "dispute notes" file.

Outcome (What the Reader Learns)

- You didn't get tricked into calling a fake support line.
- You verified in official channels first.
- You strengthened your money defenses by enabling high-signal alerts.
- If a real charge existed, you disputed quickly with documentation and a calm script—exactly as Chapter 9 teaches.

Quick “Do This Next Time” Summary

1. Verify charges in your **official bank/card app**, not email links.
2. Use the **Safer Payment Ladder** mindset (credit/wallet/virtual cards when possible).
3. Turn on the alerts that matter: online purchases, logins, new payees, transfers.
4. If needed, dispute fast: evidence + official contact + case number log.

Case Study (Chapter 9) — Meet Priya Desai: The “Refund Department” Trap and the Safer Payment Ladder

Who Priya Is

Priya Desai is a 35-year-old busy professional who pays bills online, uses a debit card for everyday purchases, and keeps a credit card “for emergencies.” She’s organized—but like most people, she doesn’t have bank alerts fully set up.

The Moment

On a Thursday afternoon, Priya gets an email with a scary subject line:

“Invoice Paid — $489.99 (Support Plan Renewal)”
Inside the email:

“If you did not authorize this charge, call our Refund Department immediately to cancel.”

Priya feels a surge of panic and thinks: *“I need to call right now before I lose money.”*

Chapter 9 is built for this exact situation: money scams that **use urgency + fake invoices** to push you into a bad decision.

Step 1 — Priya Uses the Chapter 9 Rule: Verify in the Bank App First

Instead of calling the number in the email, Priya uses the Chapter 9 approach:

- **Don’t use contact info in the message**
- **Verify inside official channels first**

She opens her bank/credit card app and checks recent transactions.

What she finds

There's a pending charge for **$489.99**—but it's on her **debit card**.

This is important because Chapter 9 explains the practical reality:

- **Debit = your money moves fast**
- **Credit = generally easier dispute leverage**

Priya realizes she needs to act quickly and carefully.

Step 2 — Priya Applies the Safer Payment Ladder (to Prevent Future Pain)

Priya decides she's going to change one habit after this:

- Use **credit** (or a digital wallet tied to credit) for online purchases and subscriptions when possible
- Keep debit for low-risk, familiar purchases
- Treat gift cards/crypto/wire requests as an automatic scam trigger

This doesn't fix today's problem yet—but it prevents the next one from draining her checking account so easily.

Step 3 — Priya Avoids the "Refund Scam Pivot"

Here's the trap: if Priya calls the "Refund Department" number from the email, a scammer often tries to pivot into one of these moves:

- "We need you to install a remote support app so we can process the refund"
- "We refunded too much—send the difference back"
- "To cancel, pay a small fee using gift cards/crypto/instant transfer"

Chapter 9 flags these as major danger signs because they push money into **irreversible channels**.

Priya makes a simple decision:
She will not call the email's number.

Step 4 — Priya Turns On the Alerts That Matter (Right Now)

Chapter 9 emphasizes catching money issues early with high-signal alerts.

Priya turns on:

- **Online/card-not-present purchase alerts**
- **ATM withdrawal alerts**
- **Login alerts**
- **New payee + outgoing transfer alerts** (if available)

She sets a small threshold so she'll notice small "test charges."

This is her "I won't be surprised again" step.

Step 5 — Priya Disputes Fast Using Official Channels + A Calm Script

Because it's debit and pending, Priya acts immediately through official bank support:

1. Calls the number on the **back of her debit card** (not the email).
2. Says a simple, clear statement:

Dispute Script (Priya uses):

"I'm reporting an unauthorized transaction for $489.99 that I did not approve. Please block the card, stop the charge if possible, and open a fraud case. Can I get the case number?"

3. She writes down:

- Case number
- Date/time
- What the bank said
- Next steps

The bank cancels the card, starts the dispute process, and confirms what to watch for next.

Step 6 — Priya Builds a “Dispute Folder” for Proof

Chapter 9 recommends keeping documentation simple and organized.

Priya saves:

- Screenshot of the transaction in her banking app
- Screenshot of the email (without clicking anything)
- A note with case number + timeline

Now if the charge posts or the bank needs follow-up, she has everything in one place.

Outcome (What Priya Learned)

Priya didn’t “win” by being technical—she won by following the Chapter 9 system:

- Verify in official channels first
- Avoid the refund trap (don’t call message numbers)
- Use alerts to catch fraud early
- Dispute quickly with a calm script and a case number
- Switch future purchases to safer payment methods

Chapter 9 in One Line

Money scams thrive on urgency—your defense is safer payment habits, high-signal alerts, and a fast, documented dispute process.

Case Study (Chapter 10): “A New Credit Inquiry You Don’t Recognize—Monitoring vs. Freeze + Identity Defense Folder”

This case study follows Chapter 10’s flow: recognize what identity theft looks like (new accounts, inquiries, address changes, tax issues), understand **monitoring vs. freeze**, apply a simple **freeze plan**, and build/use an **Identity Defense Folder** so you respond calmly instead of scrambling.

The Situation

You get an email or app alert from a credit monitoring service (or your bank) that says:

“New credit inquiry detected.”
The lender name is unfamiliar.

You haven’t applied for a credit card, car loan, apartment, or anything else recently. Chapter 10 explains this is one of the earliest signs of identity theft—someone may be trying to open credit in your name.

Step 1 — Confirm It’s Real (Don’t Assume, Don’t Panic)

Chapter 10 emphasizes: identity theft often starts small and boring. Your job is to confirm what happened.

What you do (5 minutes):

1. Open your monitoring app (or credit portal) directly—don't click random links.
2. Note the **lender name**, **date/time**, and **bureau** (if shown).
3. Check if you recently did anything that could trigger an inquiry (apartment screening, phone plan, insurance quote).

If nothing explains it, treat it as a real red flag and move to protection steps.

Step 2 — Use the Chapter 10 Map: "Monitoring vs. Freeze"

Chapter 10 teaches that these tools do different jobs:

- **Monitoring = alarms** (it tells you something happened).
- **Credit Freeze = a lock** (it blocks most new credit from being opened).

In this case, monitoring did its job by alerting you. Now you decide whether to "lock the door."

Step 3 — Decide: Do You Freeze Now?

Chapter 10 suggests a freeze is especially useful if:

- You aren't applying for new credit soon, or
- Your data may be exposed, or
- You see suspicious activity (like an unknown inquiry).

Decision in this case study:
You choose to place a **credit freeze**, because an unknown inquiry is a strong enough signal to block new-credit attempts.

Step 4 — Use a Simple Freeze Plan (So You Don't Regret It Later)

Chapter 10 recommends treating a freeze like a small system: set it, track details, and document lifts/re-freezes.

What you do (15–30 minutes):

1. Freeze your credit with the major bureaus (one by one).
2. Create logins and store them safely (password manager recommended).
3. Record any PIN/passphrase details you're given (or where you stored them).
4. Write down the date/time you froze.

This blocks most "new account" attempts while you investigate.

Step 5 — Build/Use the Identity Defense Folder (Your Calm Folder)

Chapter 10 recommends a folder (digital or physical) with the key items you'll need if anything escalates—so you don't hunt for numbers when stressed.

What you add right now:

- Official contact info for banks/cards and credit bureaus (from trusted sources)
- A simple **case log** template (date, who you spoke with, case #)
- Your account list (no passwords)
- Where backup codes/recovery methods are stored

This turns a scary moment into a manageable workflow.

Step 6 — Investigate + Clean Up (Without Doing 20 Things at Once)

Now you take the "calm next steps" Chapter 10 supports:

What you do (30–60 minutes, as able):

1. Review your credit report(s) for **new accounts** you don't recognize.
2. Watch for **address changes** or unfamiliar personal info.
3. If you find a new account you didn't open, start logging calls and case numbers in your folder.

You don't need to solve everything today; you're blocking new damage and gathering facts.

Outcome (What the Reader Learns)

- Monitoring gave you the early warning.
- A credit freeze helped block most new-credit fraud attempts.
- The Identity Defense Folder made your response organized and calm.
- You took the right-sized actions before panic could lead to mistakes.

Quick "Do This Next Time" Summary

1. Unknown inquiry = possible identity theft signal.
2. Monitoring alerts you; **freeze blocks** new credit.
3. Track freeze details like a mini system (logins/PIN + dates).
4. Use your Identity Defense Folder to log calls and case numbers.

Case Study (Chapter 10) — Meet Hannah Price: The New Account Alert

Who Hannah Is

Hannah Price is a 32-year-old nurse who keeps life simple: one main email, one bank, one credit card, and automatic bill pay. She's careful, but she assumes identity theft "happens to other people."

The Moment

On a Friday afternoon, Hannah gets an alert:

"New account opened"
It's from a credit monitoring notification. The lender name is unfamiliar, and she has not applied for any new credit.

Hannah's first reaction is panic—*"How did this happen?"*
Chapter 10 teaches the next move is not panic. It's **confirmation + containment**.

Step 1 — Hannah Identifies the Identity-Theft Signals

Chapter 10 explains the most common signs include:

- new accounts,
- new inquiries,
- address changes,
- and other unusual credit activity.

Hannah treats "new account opened" as a serious signal and decides to act the same day.

Step 2 — Hannah Verifies the Alert Using Official Channels

Before she fills out anything from the alert email, she:

- opens her monitoring portal/app directly,
- checks which bureau reported it (if shown),
- and writes down the lender name + date.

Now she has the facts without clicking suspicious links.

Step 3 — Hannah Chooses: Monitoring vs. Freeze

Chapter 10 teaches the difference:

- **Monitoring tells you** something happened.
- **A credit freeze helps prevent** most new credit from being opened.

Because Hannah is **not** planning to apply for a loan soon, she chooses the stronger protection: **freeze**.

Step 4 — Hannah Uses a Simple Credit Freeze Plan

Chapter 10 recommends treating a freeze like a mini system: set it, track details, and document actions.

Hannah:

1. Places a credit freeze with each bureau (one at a time).
2. Stores bureau logins/PIN details safely (not in plain notes).
3. Writes down the date/time she froze in a simple log.

This immediately blocks most new-credit attempts while she investigates.

Step 5 — Hannah Builds Her "Identity Defense Folder" (So She Doesn't Scramble)

Chapter 10 emphasizes an organized folder so you can respond calmly.

Hannah creates a folder (digital vault or binder) with:

- a list of official phone numbers (banks, bureaus),
- a case log template (date, who she spoke with, case #),
- her account list (no passwords),
- and where recovery/backup info is stored.

Now she has a "calm folder" for follow-up calls.

Step 6 — Hannah Documents and Starts Cleanup

Hannah checks her credit report for:

- other new accounts,
- new inquiries,
- address changes.

If she sees the suspicious account, she logs:

- lender name,
- date,
- bureau involved,
- and starts recording every contact and case number.

She doesn't try to do 20 things at once—she blocks new damage first and then works methodically.

Outcome (What Hannah Learned)

Hannah learns that identity protection is not complicated—it's procedural:

- **monitoring alerts you**,

- **freezing blocks**,
- and the **Identity Defense Folder** keeps you calm and consistent.

By acting quickly, she reduces the chance of additional accounts being opened in her name.

Chapter 10 in One Line

Monitoring is the alarm; a freeze is the lock—use both when needed, and track everything in your Identity Defense Folder.

Case Study (Chapter 11): “A Transfer You Don’t Recognize—First 15 Minutes / First 24 Hours”

This case study follows Chapter 11’s “break glass” flow: **stop communicating**, then **stop the bleeding in priority order** (bank/cards → email → phone carrier → password manager → socials), follow the **account takeover recipe**, capture **simple evidence**, and avoid the **second scam**—then stabilize within 24 hours.

The Situation

You open your banking app and see:

“Outgoing transfer: $1,250 — Pending”
You didn’t send it.

At the same time, you notice:

- A new email: **“Your email password was changed”** (you didn’t do it)
- A text: **“Your verification code is 839201”** (you didn’t request it)

Your heart starts racing. Chapter 11 is built for this moment—when it’s not “maybe,” it’s “something is happening right now.”

FIRST 15 MINUTES (Stop More Harm)

Minute 0–1: Stop Communication + Stop Sharing Info

Chapter 11 starts with the simplest rule: **stop interacting with anything that might be part of the scam** and **stop sending more info.**

What you do immediately:

- Close any suspicious emails or tabs.
- Do not reply to texts, do not call numbers from messages.
- Take one breath and commit: “I will follow the steps.”

Minute 1–6: Stop the Bleeding (Priority Order)

Chapter 11 says the order matters. You secure the accounts that move money and reset everything else.

1) Bank / Cards (money moves first)

- In the bank app: **freeze/lock cards** if available.
- If the transfer is pending: look for **cancel**, **stop transfer**, or **report fraud**.

Then call the bank using a trusted number:

- **Number on the back of your card** or inside the official app (not from email/text).

What you say (simple):

“I’m reporting an unauthorized transfer of $1,250 that I did not initiate. Please stop it if possible, lock my account, and open a fraud case. What is my case number?”

Write down the case number immediately.

Minute 6–10: Email Next (Master Key)

Chapter 11 explains why email is next: it can reset passwords for everything.

What you do:

- From a trusted device, go directly to your email provider (typed URL or official app).
- Change the email password to a new strong one.
- Review “devices/sessions” and **sign out of all other devices**.
- Check for forwarding rules/filters if available.

If you can’t log in: use the official account recovery process immediately.

Minute 10–12: Phone Carrier (SIM Swap Check)

Chapter 11 flags the carrier as priority #3 because attackers sometimes hijack your number to intercept codes.

Quick check:

- Did your phone suddenly lose service earlier?
- Did you get any carrier alerts about SIM changes?

If yes—or if you’re unsure—call carrier support using a trusted number:

“I believe my number may be under attack. Please put a lock on my account and confirm no SIM/port-out changes occurred without my authorization.”

Minute 12–15: Password Manager + Key Accounts

If you use a password manager, secure it next:

- Change the master password (if you suspect exposure)
- Sign out other sessions if that option exists

Then hit the “highest risk” accounts:

- Banking logins, payment apps, primary social accounts
- Change passwords + confirm MFA methods belong to you

EVIDENCE CAPTURE (Do this while fixing, not after)

Chapter 11 recommends simple evidence capture—enough to dispute and explain what happened.

Take screenshots of:

- The unauthorized transfer screen (amount/date/status)
- Any bank alerts/messages
- Any email security alerts (password changed, new sign-in)
- Any suspicious texts/emails involved
- Any “devices/sessions” page showing unknown devices (before you remove them)

Write down:

- When you noticed the issue (time/date)
- Amounts + transaction IDs/reference numbers
- Names/IDs of support reps and case numbers

AVOID THE “SECOND SCAM” (Most people get hit here)

Chapter 11 warns that once you’re stressed, attackers may try a second hit—fake recovery services, fake support numbers, urgent “fees,” or “hack fixers.”

Your rule for the next 24 hours:

- Only contact institutions through channels you initiate (official app, number on card, typed website).
- No one legitimate can “guarantee recovery” for a fee.

FIRST 24 HOURS (Stabilize So It Doesn't Echo)

Step 1: Update + Scan Devices

Chapter 11 recommends updating and scanning devices used during the incident.

- Install OS/browser updates
- Run reputable security scans on computer/phone

Step 2: Full Account Takeover Recipe (Repeat Everywhere)

Chapter 11 gives a standard recipe:

- Sign out of sessions
- Change password
- Verify/reset MFA methods
- Remove unknown devices/connected apps
- Check email rules/forwarding

Step 3: Credit/Identity First Steps (If Data Was Exposed)

If you entered personal info or suspect identity risk:

- Consider a fraud alert or credit freeze (as covered in Chapter 10)
- Watch for new inquiries/accounts

Step 4: Notify Contacts if Impersonation Risk

If email/social could have been used to message others:

- Send a short message: "My account was compromised. Ignore any requests for money/codes."

Step 5: Document Everything

Keep all case numbers, notes, and screenshots in one place.

- This reduces stress and improves follow-ups.

Outcome (What the Reader Learns)

This case study shows the Chapter 11 win condition: you don’t “solve” everything instantly—you **stop more harm**, regain control in the right order, capture evidence, and avoid getting hit again while you’re stressed.

Case Study (Chapter 11) — Meet Noah Jensen: The Unauthorized Transfer (First 15 Minutes / First 24 Hours)

Who Noah Is

Noah Jensen is a 39-year-old homeowner who manages everything online—banking, mortgage, utilities, and family calendars. He's not a cybersecurity person, but he's calm under pressure, and he follows checklists well.

The Moment

At 6:53 a.m., Noah checks his bank app and sees:

"Outgoing transfer: $1,980 — Pending"
He didn't send it.

At the same time:

- His email shows: **"Password reset requested"** for a payment app
- He receives an unexpected text: **"Your verification code is 773204"**

Noah feels the panic spike, but Chapter 11 trained him for this: **don't solve everything—stop more harm fast, in the right order.**

FIRST 15 MINUTES (Stop the Bleeding)

Minute 0–1: Cut Contact + Stop Guessing

Noah immediately stops interacting with anything that could be part of the scam.

- No replying to texts
- No clicking links
- No calling numbers from emails/messages

He tells himself: *“I’m switching to checklist mode.”*

Minute 1–6: Bank First (Money Moves First)

Chapter 11’s priority order starts with money. Noah opens the **official bank app** (not message links) and takes the fastest actions available:

- He taps **Freeze/Lock** card (if available)
- He looks for **Cancel/Stop transfer** (if it’s pending)

Then he calls the bank using a trusted number (back of card or in-app support).

What Noah says (calm script):

“I’m reporting an unauthorized transfer of $1,980 that I did not initiate. Please stop it if possible, lock my account, and open a fraud case. What is my case number?”

He writes down the case number immediately.

Minute 6–10: Email Next (Master Key)

Chapter 11 puts email second because it can reset everything else. Noah secures email fast:

- Changes email password to a new strong one
- Confirms MFA is on and belongs to him
- Reviews “Devices/Sessions” and signs out unknown ones
- Checks for suspicious forwarding rules/filters

This prevents the attacker from continuing to trigger password resets.

Minute 10–12: Carrier Check (SIM Swap Risk)

Chapter 11 flags the phone carrier as the next critical piece. Noah checks:

- Does his phone still have service?
- Any carrier alerts about SIM/number transfer?

Even without clear signs, he calls the carrier using an official number and asks them to:

- confirm no SIM change/port-out request occurred,
- add/verify carrier PIN and account lock if available.

Minute 12–15: Password Manager + High-Value Accounts

Now Noah secures the accounts that could be used to move more money or impersonate him:

- Password manager (if used)
- Payment apps
- Primary social accounts

He changes passwords and enables/confirms MFA where possible.

EVIDENCE CAPTURE (Quick and Practical)

Chapter 11 recommends capturing simple proof while the data is visible. Noah takes screenshots of:

- The unauthorized transfer screen (amount, status, date)
- The bank case number screen (if shown)
- Email security alerts and password reset requests
- Any suspicious messages involved

He also writes down:

- date/time noticed
- amounts
- transaction IDs/reference numbers
- who he spoke with + case #

AVOID THE “SECOND SCAM”

Right after incidents, scammers often try a second hit: fake recovery agents, paid “hack fixers,” fake support numbers, urgent fees. Noah follows Chapter 11’s rule: **only use channels you initiate** (official app, number on card, typed website).

FIRST 24 HOURS (Stabilize)

Step 1: Update + Scan Devices

Noah updates phone/computer OS, browser, and runs reputable security scans on devices used.

Step 2: Run the “Account Takeover Recipe” Everywhere

Chapter 11’s repeatable recipe:

- Sign out sessions
- Change password
- Verify/reset MFA methods
- Remove unknown devices/connected apps

- Check email rules/forwarding

Noah repeats this for email, banking, payment apps, and social accounts.

Step 3: Identity/Credit First Steps (If Needed)

If Noah entered personal info anywhere or suspects identity exposure, he begins credit/identity protections (as covered in Chapter 10).

Step 4: Notify Contacts (If Impersonation Risk)

Noah sends a short message to close contacts:

“My account may have been compromised. Please ignore any unusual messages or money requests from me.”

Step 5: Document Everything

Noah keeps one Recovery Log with:

- dates
- actions taken
- case numbers
- next steps
  This makes follow-up easier and reduces stress.

Outcome (What Noah Learned)

Noah didn’t waste time trying to “figure out the whole story.” He followed Chapter 11’s winning objective: **stop more damage first**, then stabilize and document. The checklist order (bank → email → carrier → key accounts) kept the incident from escalating.

Case Study (Chapter 12): “From Overwhelmed to Protected—Running the 30-Day AI Scam Shield Plan”

This case study follows Chapter 12’s structure exactly: use **tiny daily tasks**, build protection in layers (Week 1–4), keep AI as a helper (not a boss), and finish with a simple **maintenance rhythm** plus the “**upgrade one thing**” habit.

The Situation

Jordan is a busy adult who:

- Gets suspicious texts weekly
- Manages bills and banking online
- Feels behind on security but doesn’t have time for “tech projects”

Jordan’s goal is simple: **be much harder to scam in 30 days** without spending hours or learning jargon. Chapter 12 is designed for exactly this.

Week 1 (Days 1–7): Email + Password Manager + MFA

Goal: Secure the “keys to the kingdom” first.

Day 1 — List crown jewel accounts (5 minutes)

Jordan makes a short list (no passwords): email, bank, credit card, carrier, payment apps, primary social.

Day 2 — Install a password manager (10 minutes)

Jordan sets one strong master password and installs it on phone + computer.

Day 3 — Fix email password (10 minutes)

Jordan changes email to a strong unique password stored in the manager.

Day 4 — Turn on MFA for email (10 minutes)

Jordan enables MFA (authenticator/passkey if available) and saves backup codes securely.

Days 5–6 — Secure two money accounts (10 minutes/day)

Jordan updates passwords + enables MFA for bank and credit card logins.

Day 7 — Review + rehearse (5–10 minutes)

Jordan practices logging in using the password manager autofill and confirms backup code storage.

Result after Week 1:
Even if a scammer gets an old reused password, Jordan's email and key money accounts are much harder to take over.

Week 2 (Days 8–14): Phone + Carrier + Cleanup

Goal: Protect the phone and phone number attackers love to target.

Day 8 — Lock down the phone (5 minutes)

Strong PIN/biometric, short auto-lock, hide lock screen previews.

Day 9 — Secure the carrier account (10 minutes)

Jordan sets a carrier account PIN and requests stronger protections against number transfers/SIM swaps.

Day 10 — Turn on spam filters (5 minutes)

Jordan enables “silence unknown callers” and carrier spam filtering.

Day 11 — Notification cleanup (5 minutes)

Jordan removes sensitive message previews from lock screen.

Day 12 — Retire one old account (10 minutes)

Jordan deletes an old account or removes payment info, shrinking the attack surface.

Day 13 — Inbox cleanup (10 minutes)

Jordan unsubscribes from a few emails and creates one “Receipts & Bills” folder to reduce noise.

Day 14 — Backups on (10 minutes)

Jordan enables phone/computer backups (simple, not perfect).

Result after Week 2:
Even if someone tries a SIM swap or a phone-based scam, Jordan’s phone number and device setup are harder to exploit.

Week 3 (Days 15–21): Money Rules + Alerts + Habits

Goal: Create “money guardrails” so urgency can’t push cash out the door.

Day 15 — Write 3–5 money rules (5 minutes)

Examples:

- “I never move money based on a text/email.”

- “I call back using the number on my card.”

Day 16 — Turn on alerts (10 minutes)

Jordan enables transaction alerts, login alerts, and transfer/new-payee alerts.

Day 17 — Build a bill-pay map (10 minutes)

Jordan lists major bills and how they’re paid to spot fake “your payment failed” messages.

Day 18 — Practice the verify script (2 minutes)

Jordan practices: “I don’t handle this through links. I’ll verify in the official app.”

Day 19 — 10-minute transaction review

Jordan scans the last month for small “test charges.”

Day 20 — Automate one safer behavior (5 minutes)

Calendar reminder for weekly money review or monthly subscription cleanup.

Day 21 — Adjust for real life (5 minutes)

Jordan turns off noisy alerts and keeps the highest-signal ones.

Result after Week 3:
Jordan’s money is harder to drain quickly, and alerts catch issues early.

Week 4 (Days 22–30): Credit/Identity + Family Plan + Drill

Goal: Make identity fraud harder and rehearse what to do if something happens.

Day 22 — Pull credit baseline (15 minutes)

Jordan checks credit reports or monitoring dashboard.

Day 23 — Scan for red flags (10 minutes)

New accounts, inquiries, address changes.

Day 24 — Decide freeze vs alerts (10 minutes)

If not applying for credit soon, Jordan considers a freeze; otherwise sets alerts.

Day 25 — Family pact (10 minutes)

Household agrees:

- no codes
- no money on first call/text
- call-back rule

Day 26 — Share scripts with relatives (5 minutes)

Short note: “If I’m ‘in trouble’ and need money, hang up and call me back.”

Day 27 — 10-minute drill (10 minutes)

“What if we see a strange charge?” → bank call-back; secure email; document.

Day 28 — Build the emergency kit (10 minutes)

One secure place for official numbers + where recovery info lives.

Day 29 — Home/desk privacy sweep (10 minutes)

Remove sticky notes, store sensitive docs, reduce visible info.

Day 30 — Choose maintenance rhythm (5 minutes)

Jordan picks monthly + quarterly check-ins and commits to “upgrade one thing.”

Result after Week 4:
Jordan is not “perfectly secure,” but is now dramatically harder to scam, with a plan that actually fits real life.

The Chapter 12 “AI Assistant” Use (Correct Way)

During the 30 days, Jordan uses an AI assistant to:

- draft a call script to the bank,
- turn vague tasks into a checklist,
- summarize what to do next — **without ever pasting passwords, codes, or full account numbers.**

The Win (What the Reader Learns)

- Big security results come from **small repeated actions**.
- The plan works because it’s **tiny tasks**, not a weekend overhaul.
- After 30 days, maintenance is light: monthly check + quarterly review + “upgrade one thing.”

Case Study (Chapter 12) — Meet Rachel Knight: The 30-Day Plan That Actually Sticks

Rachel Knight is a 45-year-old working parent who's tired of feeling anxious every time her phone buzzes. She's not trying to become "tech-savvy"—she just wants to protect her money, accounts, and family with a plan she can actually finish. Chapter 12 gives her exactly that: a **30-day system** built in small steps (Week 1–4) plus a maintenance rhythm that keeps it alive.

The Moment

Rachel gets two scammy messages in one week:

- A "package delayed" text with a link
- A fake "subscription renewal invoice" email

She didn't click anything, but she realizes she's relying on luck. She decides: **"I'm doing the 30-day plan."**

Week 1: Email + Password Manager + MFA

Goal: Secure the "keys to the kingdom" first.

Day 1 — Rachel lists her "crown jewels" (5 minutes)

She writes a simple list (no passwords): email, bank, credit card, phone carrier, password manager, primary social.

Day 2 — Password manager setup (10 minutes)

She picks one password manager and creates a strong master password.

Day 3 — Email password upgrade (10 minutes)

She changes her email password to a strong unique one stored in the manager.

Day 4 — MFA for email (10 minutes)

She turns on MFA and stores backup codes securely.

Days 5–7 — Two more key accounts (10 minutes/day)

She updates and secures her bank login and her primary shopping account (because it stores payment methods).

Result after Week 1:
Even if scammers get an old password, Rachel's email and money accounts are much harder to take over.

Week 2: Phone + Carrier Protections + Cleanup

Goal: Protect the phone number and device scammers use to intercept codes.

Day 8 — Phone lock + settings (10 minutes)

She sets a 6+ digit PIN, enables auto-lock, and hides lock-screen previews (so codes aren't visible).

Day 9 — Carrier protection (15 minutes)

Rachel calls her carrier and adds a **carrier PIN** and a **port-out/SIM-change lock**.

Day 10 — App cleanup (10 minutes)

She deletes unused apps and removes any that look sketchy or unnecessary.

Days 11–14 — Update habits (5–10 minutes/day)

She turns on automatic updates for her phone and apps and sets a reminder to review permissions monthly.

Result after Week 2:
SIM swap and “code interception” becomes much harder, and her phone is less vulnerable to common tricks.

Week 3: Money Rules + Alerts + Routine

Goal: Catch fraud early and reduce “fast money loss.”

Day 15 — Rachel writes 3 money rules (5 minutes)

- “I never pay from a text link.”
- “I call back using the number on my card.”
- “No gift cards, crypto, or wire transfers.”

Day 16 — Alerts that matter (15 minutes)

She enables alerts for: online transactions, logins, new payees, and outgoing transfers.

Days 17–21 — Weekly money habit (10 minutes total)

Rachel does her first weekly routine: review transactions, check alerts, and make one improvement (like removing saved cards from a rarely-used account).

Result after Week 3:
She’s far less likely to miss “test charges” or an early warning sign.

Week 4: Credit/Identity + Family Pact + Drill

Goal: Make identity fraud harder and rehearse what to do under stress.

Day 22 — Quick credit check (15 minutes)

She checks for unfamiliar inquiries or new accounts.

Day 23 — Monitoring vs. freeze decision (10 minutes)

She chooses whether to freeze credit now (if she's not applying for new credit soon) or strengthen monitoring alerts.

Day 24 — Identity Defense Folder (15 minutes)

She creates a "calm folder" with official contact numbers, a simple case log template, and where recovery info lives.

Day 25 — Family pact (10 minutes)

Rachel teaches her household:

- no codes
- no money on first call/text
- call-back rule
- family code word

Day 26 — 10-minute drill

"What if we see a strange transfer?" → bank call-back → secure email → document.

Result after Week 4:
Rachel isn't just "safer"—she's prepared and calm, with a system the whole household understands.

The "Make It Stick" Part (After Day 30)

Chapter 12 says the plan stays alive with two simple practices:

1. **Monthly check-in** (10 minutes): alerts + transactions + one account review
2. **Quarterly review** (20 minutes): sessions/devices + recovery info + family reminder
3. **Upgrade one thing** each month (one small improvement, no overwhelm)

Rachel chooses one monthly upgrade: adding MFA to one more account or removing an outdated recovery number.

What Rachel Learned (Chapter 12 in One Line)

Security becomes real when it becomes routine—tiny steps, done consistently, beat big plans you never finish.

Conclusion

If there's one thing you should take from this Case Study Workbook, it's this: **you don't need to be a tech expert to be hard to scam**. What protects you isn't perfect knowledge—it's having a simple system you can run even when you're busy, tired, or stressed.

Across these case studies, you practiced the same winning pattern again and again:
Pause → Verify → Decide.
You learned to identify what a scammer is really after (money, accounts, identity, or access), spot the emotional pressure that tries to rush you, and shift the conversation into **official channels you control**. You also learned the right way to use AI assistants: as a calm helper for clarity and scripts—not as a vault and not as a guarantee.

Just as important, you built "real life" defenses that compound over time: securing email (the master key), hardening your phone and carrier protections, setting money alerts, understanding credit monitoring versus freezes, and following the right order when something goes wrong. And you saw how protection becomes sustainable when it's broken into small habits—especially the 30-day plan and the "upgrade one thing" mindset.

As you finish this workbook, don't aim for perfection. Aim for consistency. Pick one case study and run it again with a family member. Save your scripts. Print your key checklists. Then keep your system alive with a simple monthly check-in. The goal is not to live in fear—it's to live with confidence.

You're not powerless in a world of smarter scams. You have a plan. And now you've practiced it.